PCT/JP2004/016708

日本国特許庁
JAPAN PATENT OFFICE

04.11.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月１３日

出願番号
Application Number: 特願２００４－０３７３１４

[ST. 10/C]: [ＪＰ２００４－０３７３１４]

出願人
Applicant(s): エヌ・ティ・ティ・コミュニケーションズ株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００４年１２月１３日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１１３６６１

【書類名】　特許願
【整理番号】　GLN00462
【提出日】　平成16年 2月13日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 17/00
H04L 12/22

【発明者】
【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】　齊藤　充

【発明者】
【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】　山崎　俊之

【発明者】
【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】　宮川　晋

【発明者】
【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】　江頭　孝

【発明者】
【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】　鈴木　俊明

【発明者】
【住所又は居所】　東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
【氏名】　内山　貴充

【特許出願人】
【識別番号】　399035766
【氏名又は名称】　エヌ・ティ・ティ・コミュニケーションズ株式会社

【代理人】
【識別番号】　100070150
【弁理士】
【氏名又は名称】　伊東　忠彦

【手数料の表示】
【予納台帳番号】　002989
【納付金額】　21,000円

【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
第１の装置及び第２の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、
第１の装置との間で相互認証を行い、セッション管理装置と第１の装置との間で第１の暗号化通信チャネルを確立し、第１の装置の名前と第１の暗号化通信チャネルの識別情報とを対応付けて保持する手段と、
セッション管理装置と第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立する手段と、
第１の装置から、第１の装置の名前を含むメッセージを、第１の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第１の装置の名前と、第１の暗号化通信チャネルの識別情報と対応付けて保持されている第１の装置の名前とを比較することにより、メッセージに含まれる第１の装置の名前が正しいか否かを判定する手段と、
そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信する手段と
を有することを特徴とするセッション管理装置。
【請求項２】
前記メッセージに含まれる第１の装置の名前が正しくないと判定した場合に、エラーメッセージを第１の装置に送信する請求項１に記載のセッション管理装置。
【請求項３】
第１の装置及び第２の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、
第１の装置との間で相互認証を行い、セッション管理装置と第１の装置との間で第１の暗号化通信チャネルを確立する手段と、
セッション管理装置と第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立する手段と、
第１の装置から、第１の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第１の暗号化通信チャネルを介して受信する手段と、
セッション管理装置と第２の装置との間の経路の信頼性を示すヘッダを前記メッセージに追加し、そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信する手段と
を有することを特徴とするセッション管理装置。
【請求項４】
前記メッセージに含まれる前記経路の信頼性を示すヘッダは、当該ヘッダを付した装置のアドレスを含み、当該メッセージを受信すると、そのヘッダに含まれるアドレスと、当該メッセージを送信した送信元の装置のアドレスとを比較することにより、当該ヘッダの正当性を判定する請求項３に記載のセッション管理装置。
【請求項５】
前記メッセージはＳＩＰに基づくメッセージである請求項１ないし４のうちいずれか１項に記載のセッション管理装置。
【請求項６】
ネットワークに接続された第１の装置、セッション管理装置、及び第２の装置の間でメッセージを転送する方法であって、
セッション管理装置と第１の装置との間で相互認証を行い、セッション管理装置と第１の装置との間で第１の暗号化通信チャネルを確立し、セッション管理装置が、第１の装置の名前と第１の暗号化通信チャネルの識別情報とを対応付けて保持するステップと、
セッション管理装置と第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立するステップと、
第１の装置が、第１の装置の名前を含むメッセージを第１の暗号化通信チャネルを介してセッション管理装置に送信するステップと、
セッション管理装置が、前記メッセージに含まれる第１の装置の名前と、第１の暗号化

通信チャネルの識別情報と対応付けて保持されている第１の装置の名前とを比較することにより、前記メッセージに含まれる第１の装置の名前が正しいか否かを判定するステップと、
そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信するステップと
を有することを特徴とする方法。
【請求項７】
セッション管理装置は、前記メッセージに含まれる第１の装置の名前が正しくないと判定した場合に、エラーメッセージを第１の装置に送信する請求項６に記載の方法。
【請求項８】
ネットワークに接続された第１の装置、セッション管理装置、及び第２の装置の間でメッセージを転送する方法であって、
セッション管理装置と第１の装置との間で相互認証を行い、セッション管理装置と第１の装置との間で第１の暗号化通信チャネルを確立するステップと、
セッション管理装置と第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立するステップと、
第１の装置が、第１の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第１の暗号化通信チャネルを介してセッション管理装置に送信するステップと、
セッション管理装置が、セッション管理装置と第２の装置との間の経路の信頼性を示すヘッダを追加した前記メッセージを第２の暗号化通信チャネルを介して第２の装置に送信するステップと
を有することを特徴とする方法。
【請求項９】
第２の装置は、前記メッセージに付された経路の信頼性を示すヘッダを参照して、前記メッセージが信頼できるものであるか否かの判定を行う請求項８に記載の方法。
【請求項１０】
第２の装置は、当該第２の装置が受信したメッセージに付された経路の信頼性を示す一連のヘッダと同じ一連のヘッダを含む応答メッセージを前記セッション管理装置に送信する請求項８又は９に記載の方法。
【請求項１１】
前記メッセージに含まれる前記経路の信頼性を示すヘッダは、当該ヘッダを付する装置のアドレスを含み、当該メッセージを受信した装置は、そのヘッダに含まれるアドレスと、当該メッセージを送信した送信元の装置のアドレスとを比較することにより、当該ヘッダの正当性を判定する請求項８に記載の方法。
【請求項１２】
前記メッセージはＳＩＰに基づくメッセージである請求項６ないし１１のうちいずれか１項に記載の方法。
【請求項１３】
コンピュータを、ネットワークに接続された第１の装置と第２の装置との間でメッセージ送受信を行うセッション管理装置として機能させるプログラムであって、コンピュータを、
第１の装置との間で相互認証を行い、第１の装置との間で第１の暗号化通信チャネルを確立し、第１の装置の名前と第１の暗号化通信チャネルの識別情報とを対応付けて保持する手段、
第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立する手段、
第１の装置から、第１の装置の名前を含むメッセージを、第１の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第１の装置の名前と、第１の暗号化通信チャネルの識別情報と対応付けて保持されている第１の装置の名前とを比較することにより、メッセージに含まれる第１の装置の名前が正しいか否かを判定する手段、
そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信する手段

として機能させるプログラム。

【請求項１４】

コンピュータを、ネットワークに接続された第１の装置と第２の装置との間でメッセージ送受信を行うセッション管理装置として機能させるプログラムであって、コンピュータを、

第１の装置との間で相互認証を行い、第１の装置との間で第１の暗号化通信チャネルを確立する手段、

第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立する手段、

第１の装置から、第１の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第１の暗号化通信チャネルを介して受信する手段、

第２の装置との間の経路の信頼性を示すヘッダを前記メッセージに追加し、そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信する手段

として機能させるプログラム。

【書類名】明細書
【発明の名称】端末間の暗号化通信チャネルを構築するためのセッション管理装置、方法及びプログラム
【技術分野】
【０００１】
本発明は、ネットワーク上の２つの端末間でセキュアなデータチャネルを構築する技術に関するものである。
【背景技術】
【０００２】
従来技術において、ＩＰネットワーク上の２つの端末間でデータチャネルを構築しいわゆるピア・ツー・ピアの通信を行うためには、ＤＮＳへの名前登録から、セキュリティを確保するためのＦＷ等の設定・管理、証明書の取得等の作業が必要である。また、多数の端末同士の間で相互認証および暗号化されたピア・ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のＩＤ、パスワードを管理することが必要である。
【０００３】
また、従来技術として、ＳＩＰに基づくシグナリングを行って、２端末間でデータチャネルを確立する技術があるが、このような従来技術において両端末が互いを信頼しながらシグナリングできるようにするためには、例えば両端末間で予め証明書と鍵情報を交換しておくという煩雑な手続きが必要である。
【０００４】
上記の通り、従来技術ではセキュアなデータチャネルを容易に構築することはできなかった。
【特許文献１】特開２００２－２０８９２１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
本発明は、上記の点に鑑みてなされたものであり、安全にシグナリングを行って端末間でセキュアなデータチャネルを容易に構築するための技術を提供することを目的とする。
【課題を解決するための手段】
【０００６】
上記の課題は、第１の装置及び第２の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、第１の装置との間で相互認証を行い、セッション管理装置と第１の装置との間で第１の暗号化通信チャネルを確立し、第１の装置の名前と第１の暗号化通信チャネルの識別情報とを対応付けて保持する手段と、セッション管理装置と第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立する手段と、第１の装置から、第１の装置の名前を含むメッセージを、第１の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第１の装置の名前と、第１の暗号化通信チャネルの識別情報と対応付けて保持されている第１の装置の名前とを比較することにより、メッセージに含まれる第１の装置の名前が正しいか否かを判定する手段と、そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信する手段とを有することを特徴とするセッション管理装置によって解決できる。
【０００７】
本発明によれば、端末が名前を詐称することを防止することができ、安全にメッセージを転送できる。これにより、シグナリングメッセージを安全に転送でき、また、シグナリングメッセージに端末間通信のための鍵情報を含めることにより、端末間でセキュアなデータチャネルを容易に構築することができる。
【０００８】
前記メッセージに含まれる第１の装置の名前が正しくないと判定した場合に、エラーメッセージを第１の端末に送信するようにしてもよい。

【０００９】
また、上記の課題は、第１の装置及び第２の装置とネットワークを介して接続する手段を備えたセッション管理装置であって、第１の装置との間で相互認証を行い、セッション管理装置と第１の装置との間で第１の暗号化通信チャネルを確立する手段と、セッション管理装置と第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立する手段と、第１の装置から、第１の装置とセッション管理装置間の経路の信頼性を示すヘッダを含むメッセージを、第１の暗号化通信チャネルを介して受信する手段と、セッション管理装置と第２の装置との間の経路の信頼性を示すヘッダを前記メッセージに追加し、そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信する手段とを有することを特徴とするセッション管理装置によっても解決できる。

【００１０】
本発明によれば、経路の信頼性を示すヘッダをメッセージに含めるので、メッセージを受信した第２の装置では、ヘッダを確認することにより、経路の信頼性を確認でき、結果としてメッセージの信頼性を確認できる。従って、安全にシグナリングメッセージを転送できる。

【００１１】
前記メッセージに含まれる前記経路の信頼性を示すヘッダは、当該ヘッダを付した装置のアドレスを含み、当該メッセージを受信すると、そのヘッダに含まれるアドレスと、当該メッセージを送信した装置のアドレスとを比較することにより、当該ヘッダの正当性を判定するようにしてもよい。

【発明の効果】

【００１２】
本発明によれば、名前の詐称を防止し、経路の信頼性を確保ながら安全にシグナリングを行って端末間でセキュアなデータチャネルを容易に構築することができる。

【発明を実施するための最良の形態】

【００１３】
以下、本発明の実施の形態を図を参照して説明する。

【００１４】
まず、図１を用いて本発明の実施の形態の概要について説明する。

【００１５】
図１に示すように、端末１と端末２との間にセッション管理サーバ３を設置し、端末１－セッション管理サーバ３－端末２間で、端末１－端末２間のデータチャネル構築のためのシグナリング（信号手順）を実行し、データチャネル構築後はセッション管理サーバ３を介さずに端末間のみでデータ通信を行うというものである。

【００１６】
シグナリングにおいては、まず、端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間の各々で、ＩＰｓｅｃ等の暗号化通信を行うためのセキュアシグナリングチャネル確立のために、暗号鍵情報の交換、相互認証が行われる。そして、端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間の各々で確立されたセキュアシグナリングチャネルを介してセッション管理サーバへの名前登録、端末１－端末２間のセキュアデータチャネル確立のためのシグナリングが実行される。

【００１７】
端末１－セッション管理サーバ３間、セッション管理サーバ３－端末２間でのセキュアシグナリングチャネル確立におけるシグナリングにより、セッション管理サーバ３と端末１との間、セッション管理サーバ３と端末２との間において相互認証に基づく信頼関係が確立されているため、端末１と端末２との間でも信頼関係が確立されている。すなわち、上記の相互認証により、セッション管理サーバ３を介した信頼のチェーンモデルが構築される。従って、端末１－端末２間のセキュアデータチャネル確立のためのシグナリングでは、簡易な鍵情報の交換手順を用いることができる。

【００１８】

次に、端末１－セッション管理サーバ３－端末２間の通信のシーケンスを図２を参照して説明する。

【００１９】

図２に示すシーケンスは、端末１、セッション管理サーバ３、端末２がインターネット等のＩＰネットワークに接続されたシステム構成を前提とするものである。

【００２０】

各端末は、セッション管理サーバ３との間でシグナリングを実行するシグナリング機能、セキュアデータチャネルを介してデータ通信を行うための機能、及びデータ通信を利用して所望のサービスを提供するアプリケーションを備えている。

【００２１】

また、セッション管理サーバは、シグナリングを各端末との間で実行するシグナリング機能、端末間の接続許可等を制御する接続ポリシー制御機能、各端末を認証するための認証機能、端末の名前からＩＰアドレスを取得する名前解決機能、及び、認証のために用いるＩＤ、パスワードを格納するデータベースや、名前とＩＰアドレスを対応付けて格納するデータベース等を備えている。また、名前解決機能として一般のＤＮＳと同等の機能を持たせることもできる。

【００２２】

図２に示すように、端末１－端末２間でのセキュアデータチャネル構築にあたり、まず、端末１－セッション管理サーバ３間、端末２－セッション管理サーバ３間の各々でセキュアシグナリングチャネルを構築して、名前の登録を行う。

【００２３】

すなわち、端末１－セッション管理サーバ３間でＩＰｓｅｃ等の暗号通信で用いる鍵情報（暗号鍵生成用の情報）の交換を行う（ステップ１）。その後、自分のＩＤ、パスワードを含む情報を暗号化して相手側に送信することにより、相互に認証を行う（ステップ２）。認証後は、セキュアシグナリングチャネルが確立された状態となり、そのチャネルを用いて、端末１は名前とＩＰアドレスの登録をセッション管理サーバ３に対して行う（ステップ３）。端末１の通信相手となる端末２とセッション管理サーバ３間でも同様のシーケンスが実行され、端末２の名前とＩＰアドレスがセッション管理サーバ３に登録される（ステップ４、５、６）。

【００２４】

その後、端末１から端末２への接続要求が、セキュアシグナリングチャネルを介して送信される（ステップ７）。接続要求には、端末２の名前と暗号通信用の鍵情報（暗号鍵生成用の情報）が含まれる。接続要求を受信したセッション管理サーバ３は、端末１からの接続要求に関して、端末１が嘘をついていないことをチェックし（発信者詐称チェック）、更に、接続ポリシー制御機能を用いて端末１と端末２の接続が許可されているかをチェックし（ステップ８）、許可されていれば、名前解決機能を用いてデータベースを参照することにより端末２の名前から端末２のＩＰアドレスを取得し（ステップ９）、セキュアシグナリングチャネルを介して端末２へ接続要求を転送する（ステップ１０）。このとき、端末１のＩＰアドレスも端末２に送信される。端末１と端末２の接続が許可されていなければ、端末１の接続要求は拒否される。このとき、端末２に関する情報は端末１には全く送信されない。発信者詐称チェックについては後により詳細に説明する。

【００２５】

接続要求を受信した端末２は、接続要求に対する応答として、暗号通信用の鍵情報を含む応答メッセージをセキュアシグナリングチャネルを介してセッション管理サーバ３に送信し（ステップ１１）、セッション管理サーバ３がその応答メッセージを端末１に送る（ステップ１２）。このとき、端末２のＩＰアドレスも端末１に送信される。

【００２６】

この手順により、端末１と端末２との間での暗号化通信が可能となる。すなわち、セキュアデータチャネルが確立され、所望のデータ通信が行われる。

【００２７】

ステップ１、２及び４、５を経てセキュアシグナリングチャネルが確立されているということは、端末－セッション管理サーバ間で相互に認証が成功しており、信頼関係が成立しているということである。端末１－セッション管理サーバ３間、及び端末２－セッション管理サーバ３間の各々でこのような関係が成立しているので、端末１と端末２との間も相互に信頼できる関係となることから、ステップ７以降は、一般の暗号化通信で用いられる鍵交換手順より簡略化した手順を用いることが可能となっている。

【００２８】

上記のシーケンスを実現する手段として、ＳＩＰ（session initiation protocol）を拡張したプロトコルを用いることが可能である。すなわち、セッション管理サーバ３をＳＩＰプロキシサーバとして機能させ、ＳＩＰのメッセージに上記の手順でやり取りされる情報を含ませる。

【００２９】

この場合、セキュアシグナリングチャネルの確立及び名前登録のためにＲＥＧＩＳＴＥＲメッセージを用い、端末１－端末２間のセキュアデータチャネル確立のためにＩＮＶＩＴＥメッセージを用いることができる。

【００３０】

ＳＩＰを用いる場合のシーケンス例を図３に示す。

【００３１】

図３に示す例は、セキュアなチャネルで接続された複数のセッション管理サーバを経由してシグナリングを行う場合の例である。なお、セキュアなチャネルで接続された複数のセッション管理サーバをセッション管理装置と称する場合がある。図３に示すシーケンスの構成において、端末１のＩＰアドレスが２００１：１２３４：：１０、セッション管理サーバＡのＩＰアドレスが２００１：６７８９：：５０６０、セッション管理サーバＢのＩＰアドレスが２００１：ａｂｃｄ：：５０６０、端末２のＩＰアドレスが２００１：ｃｄｅｆ：：１０である。

【００３２】

各端末とセッション管理サーバ間では予め互いにＩＤ、パスワードを配布しておき、端末とセッション管理サーバの各々は、相手のＩＤ、パスワードを自分の記憶装置に格納する。また、セッション管理サーバＡとセッション管理サーバＢの間は、ＴＬＳ等のセキュアなチャネルを介して通信を行う。

【００３３】

まず、端末１、２は、ＲＥＧＩＳＴＥＲメッセージを用いて、セッション管理サーバとのセキュアチャネルの確立、及び、（ＳＩＰに準拠した）名前の登録をセッション管理サーバＡ、Ｂに対して行う（ステップ２１）（図２のステップ１～６に相当する）。なお、この部分の手順については後により詳細に説明する。

【００３４】

続いて、端末１が、暗号通信用の鍵情報（図の例では秘密共有鍵生成用の情報）をＳＤＰパラメータとして記述したＩＮＶＩＴＥメッセージを、端末２への接続要求として、端末１とセッション管理サーバＡ間のセキュアシグナリングチャネルを介して送信する（ステップ２２）。セッション管理サーバＡは、そのＩＮＶＩＴＥメッセージをセッション管理サーバＡ、Ｂ間のセキュアなチャネルを介してセッション管理サーバＢに転送する（ステップ２３）。

【００３５】

なお、端末１からのＩＮＶＩＴＥメッセージにはRoute-Securityヘッダが含まれる。Route-Securityヘッダが付加されている場合、そのＩＮＶＩＴＥメッセージを受信した装置は、Route-Securityヘッダ：[アドレス]で示されているアドレスから当該装置までの経路がセキュアなものであるかとうか（例えばＩＰｓｅｃによる暗号化がなされているかどうか）をチェックし、セキュアなものであればそのRoute-Securityヘッダをそのまま残してメッセージを転送する。また、転送先で経路がセキュアなものであるかとうかチェックを要する場合には、Route-Securityヘッダ：[自分のアドレス]を付加したメッセージをその

転送先に転送する。応答メッセージには、これまでに付されたRoute-Securityヘッダがそのまま付されており、これにより、メッセージがセキュアな経路を介して転送されたものであることがわかる。すわわち、Route-Securityヘッダにより、経路の安全性を担保する仕組みが提供される。なお、Route-Securityヘッダの種々の形態については後により詳細に説明する。

【００３６】

セッション管理サーバＢは端末２に、ＩＮＶＩＴＥメッセージを端末２とセッション管理サーバＢ間のセキュアシグナリングチャネルを介して送信する（ステップ２４）。なお、セッション管理サーバＡ及びセッション管理サーバＢにおいて端末２の名前解決がなされている。

【００３７】

ＩＮＶＩＴＥメッセージを受信した端末２は、暗号通信用の鍵情報をＳＤＰパラメータとして含む応答メッセージを端末１に向けて送信する（ステップ２５）。そして、その応答メッセージは、ＩＮＶＩＴＥメッセージと同じルート上を逆の方向に運ばれ、端末１に送信される（ステップ２６、２７）。

【００３８】

その後、受信確認（ＡＣＫ）メッセージが端末１から端末２に送信され（ステップ２８～３０）、端末１と端末２との間の暗号化通信（例えばＩＰｓｅｃによる通信）が可能となる。

【００３９】

図３のステップ２１におけるＲＥＧＩＳＴＥＲメッセージのシーケンスは、例えば図４に示す通りである。

【００４０】

この場合、まず、暗号通信用（ＩＰｓｅｃ等）の鍵情報を含むＲＥＧＩＳＴＥＲメッセージを端末からセッション管理サーバに送信する（ステップ２１１）。セッション管理サーバはその応答として暗号通信用の鍵情報を含む応答メッセージを端末に返す（ステップ２１２）。続いて、端末は、セッション管理サーバが端末を認証するための認証用情報を含むＲＥＧＩＳＴＥＲメッセージをセッション管理サーバに送信する（ステップ２１３）。セッション管理サーバはその応答として、端末がセッション管理サーバを認証するために必要な認証用情報を含む応答メッセージを端末に送信する（ステップ２１４）。互いの認証が取れた後、セキュアシグナリングチャネルによる暗号化通信が可能となる。

【００４１】

その後は、パケットがセキュアシグナリングチャネルを介して暗号化して送受信されるため、通常のＲＥＧＩＳＴＥＲメッセージシーケンスにより名前の登録が行われる（ステップ２１５、２１６）。

【００４２】

なお、上記のシーケンスにおいて、ＩＰｓｅｃ等の暗号化通信に必要なその他の情報は適宜送受信されているものとする。なお、認証用情報は、ＩＤ、パスワード等を含む情報でもよいし、証明書（Ｘ．５０９証明書等）でもよい。また、暗号通信用の鍵情報の交換のために用いるメッセージに認証用情報（証明書）を含めてもよい。

【００４３】

（身元詐称監視、ルートの信頼性確認）

さて、これまでに説明したように、端末とセッション管理サーバ間で相互認証を行うことにより、各端末とセッション管理サーバとの間で相互信頼の関係が築け、これにより、セッション管理サーバを介した簡易なシグナリング手順を用いて端末間でセキュアデータチャネルを容易に確立できるようになる。更に本実施の形態では、図３に示したシーケンスにおいて、セキュアデータチャネル構築におけるＩＮＶＩＴＥメッセージによるシグナリングをよりセキュアに行うために、セッション管理サーバによる身元詐称監視（発信者詐称チェック）、及び、ルートが安全であることを通知するためのRoute-Securityヘッダの付加を行っている。

【００４４】
ここで、Route-Securityヘッダについて説明する。前述したように、Route-Securityヘッダは、ＩＮＶＩＴＥメッセージ等のリクエストメッセージの送信の際に、端末（ＳＩＰＵＡ）、及び各セッション管理サーバ（ＳＩＰプロキシ）にて付加されるヘッダであり、少なくとも自身のＩＰアドレスを含む。Route-Securityヘッダは、リクエストメッセージの送信に用いる経路（リンクともいう）がセキュアなものであることを送信先に通知する場合に付加する。また、リクエストメッセージを送信しようとするリンクのセキュリティが予め定めたレベル以上である場合に付加するようにしてもよい。

【００４５】
Route-Securityヘッダには、リクエストメッセージを次のノードに送信するために用いるリンクのセキュリティ機能に応じた“セキュリティレベル”のパラメータを付加してもよい。例えば、認証（本人性確認）を行わない、認証行う、完全性保証（パケットが改ざんされていないことを保証）、秘密性（パケットの内容を暗号化）、等のレベルに応じて、０～３のパラメータを付加することができる。セキュリティレベル付きのメッセージを受信したノードは、Route-SecurityヘッダのＩＰアドレスと、前段ノードのＩＰアドレスとを比較することにより、Route-Securityヘッダが正しく付加されているか否かを判定できるとともに、Route-Securityヘッダに示されたセキュリティレベルが、メッセージを受信したリンクのセキュリティレベルと一致するか否かにより、パラメータが正当なものか否かを判定できる。なお、Route-SecurityヘッダのＩＰアドレスと、前段のＩＰアドレスとが一致していない場合に、前段でRoute-Securityヘッダが付加されていなかったものと判定し、前段のＩＰアドレスを使用して“セキュリティレベル”無しのRoute-Securityヘッダを追加するようにしてもよい。これにより、受信端末で、Route-Securityヘッダが付加されなかったリンクがあることを知ることができる。

【００４６】
１つ又は複数のセッション管理サーバを経由してリクエストメッセージを受信した端末（ＳＩＰ　ＵＡ）は、メッセージに付加されているRoute-Securityヘッダを参照することにより、例えば、経路中にRoute-Securityヘッダが付加されていないリンクが存在する場合に、安全性の十分でない経路を経由した可能性があることを判断できる。また、セキュリティレベルの低いパラメータを有するRoute-Securityヘッダが含まれている場合、セキュリティレベルが低いリンクを経由したことを判定できる。信頼性が十分でないと判定した場合、例えばエラー応答を返すことができる。

【００４７】
また、一連の相互認証に基づくセキュアシグナリングチャネルを介してリクエストメッセージが端末に転送される場合には、各ノードは、前段のノードが正しくRoute-Securityヘッダを付加したか否かをチェックする（例えば、IPアドレスをチェックする）だけでもよい。すなわち、一連のRoute-Securityヘッダが付加されたリクエストメッセージを受信した端末は、その前段のノードが付加したRoute-Securityヘッダをチェックするのみで経路の安全性を信頼する。この場合、例えば、各ノードでは、前段で正しいRoute-Securityヘッダが付加されていないことを検出した場合には、送信元にエラーを返すなどの処理を行う。後に説明する図５、６、７に示す例は、この場合を示している。

【００４８】
さて、リクエストメッセージを受信した端末は、受信したリクエストメッセージに含まれるRoute-Securityヘッダを、順序を維持した上でそのまま応答メッセージに含める。応答メッセージは、リクエストメッセージと同じ経路で送信元の端末に転送されるが、経由する各セッション管理サーバでは、例えば、自身が付与したRoute-Securityヘッダに含まれるＩＰアドレスを、自身のＩＰアドレスと比較することにより、メッセージをチェックできる。

【００４９】
Route-Securityヘッダがそのまま付加された応答メッセージを受信したリクエストメッセージ送信元の端末は、リクエストメッセージを受信した端末と同様にして一連のRoute-

Securityヘッダをチェックすることによりメッセージの信頼性を判定でき、例えば、信頼性が低いと判定した場合にセッションを取りやめることができる。

【００５０】

なお、一連の相互認証に基づくセキュアシグナリングチャネルを介してリクエストメッセージが端末に転送される場合には、自身のアドレスが含まれるRoute-Securityヘッダをチェックするのみでもよい。

【００５１】

次に、セッション管理サーバによる身元詐称監視、及び、Route-Securityヘッダの使用例について説明するために、図３に示したシーケンスにおけるステップ２２～ステップ２７の部分の処理をより詳細に説明する。

【００５２】

図５にそのシーケンスを示す。図６、７は、図５に示すシーケンスを説明するための図である。以下の説明では、端末１とセッション管理サーバＡ間、及び端末２とセッション管理サーバＢ間でのセキュアシグナリングチャネル確立、及び名前とアドレスのセッション管理サーバへの登録は済んでいるものとする（図５のステップ５１～５４）。

【００５３】

まず、図６（ａ）に示すように、ＩＮＶＩＴＥメッセージがセッション管理サーバＡに対して送信される（ステップ５５）。ＩＮＶＩＴＥメッセージには、端末１のＩＰアドレスを含むRoute-Securityヘッダと、接続先（端末２）の名前（Ｔｏ行、user-b@xyz.com）と、送信元（端末１）の名前（Ｆｒｏｍ行、user-a@abc.com）を含む。

【００５４】

図６（ｂ）に示すように、ＩＮＶＩＴＥメッセージを受信したセッション管理サーバＡは、Ｆｒｏｍ行にある端末１の名前が正しいか否か（詐称されていないか否か）をチェックする。ここで、セッション管理サーバＡは、端末１の名前、ＩＰアドレス、ポート番号、端末１とセッション管理サーバＡ間のセキュアシグナリングチャネルのコネクションを識別する情報（例えばＩＰｓｅｃＳＡ）を対応付けて保持している。従って、セッション管理サーバＡは、ＩＮＶＩＴＥメッセージを受信したコネクション、送信元のＩＰアドレス等から、ＩＮＶＩＴＥメッセージの送信元の名前を把握でき、その名前と、受信したＩＮＶＩＴＥメッセージのＦｒｏｍ行にある名前とを比較して、これらが一致した場合に詐称はないものと判断できる。また、同様に、Route-Securityヘッダに含まれるＩＰアドレスと、上記のコネクションに対応するＩＰアドレスとを比較して、Route-Securityヘッダが正しく付加されているか否かを判断できる。ここでＦｒｏｍ行もしくはRoute-Securityヘッダが正しくないものである場合には、例えばＩＮＶＩＴＥメッセージの転送を止め、エラーメッセージを送信元に返すこと等が可能である。

【００５５】

なお、端末１とセッション管理サーバＡ間では相互認証がなされた上でセキュアシグナリングチャネルが設けられているので、セッション管理サーバＡは、端末１から受信するＩＮＶＩＴＥメッセージを端末１から送信されたものであると信頼できる。従って、Ｆｒｏｍ行にある名前をチェックすることにより、端末１が詐称を行っていないかどうかをチェックできる。

【００５６】

次に、セッション管理サーバＡは、自身のＩＰアドレスを含むRoute-Securityヘッダを追加したＩＮＶＩＴＥメッセージをセッション管理サーバＢに転送する（ステップ５６）。セッション管理サーバＡとセッション管理サーバＢ間も端末１とセッション管理サーバＡ間と同様にセキュアなチャネルで接続されており、セッション管理サーバＢは、セッション管理サーバＡからそのチャネルを介して送られてきたＩＮＶＩＴＥメッセージは確かにセッション管理サーバＡから送られてきたものであると判断する。そして、セッション管理サーバＢは、セッション管理サーバＡにおいて追加されたRoute-SecurityヘッダのＩＰアドレス等をチェックすることにより、Route-Securityヘッダが正しく付加されているか否かをチェックする。

【００５７】
続いて、図７（ａ）に示すように、セッション管理サーバＢは、自身のＩＰアドレスを含むRoute-Securityヘッダを追加したＩＮＶＩＴＥメッセージを端末２に転送する（ステップ５７）。端末２は、Route-Securityヘッダをチェックすることにより、ＩＮＶＩＴＥメッセージが転送されてきた経路の信頼性を確認できる。
【００５８】
ＩＮＶＩＴＥメッセージを受信した端末２は、Route-Securityヘッダと、Ｔｏ行、Ｆｒｏｍ行をそのまま含む応答メッセージを、ＩＮＶＩＴＥメッセージが転送されてきた経路と逆の経路を辿って送信元に送信する。従って、まず、応答メッセージはセッション管理サーバＢに送信される（ステップ５８）。
【００５９】
端末２から応答メッセージを受信したセッション管理サーバＢは、例えば、先頭のRoute-Securityヘッダのアドレスが自身のＩＰアドレスと一致するか否かを判断することによってメッセージの詐称チェックを行う。そして、応答メッセージはセッション管理サーバＢからセッション管理サーバＡに転送される（ステップ５９）。
【００６０】
セッション管理サーバＡでは、２番目のRoute-Securityヘッダのアドレスが自身のＩＰアドレスと一致するか否かを判断することによってチェックを行う。そして、応答メッセージは、ＩＮＶＩＴＥメッセージの送信元である端末１に転送され（ステップ６０）、端末１では、３番目のRoute-Securityヘッダのアドレスが自身のＩＰアドレスと一致するか否かを判断することによってメッセージの正当性をチェックする。また、端末１は、一連のRoute-Securityヘッダを確認することにより経路の信頼性を確認することもできる。ここで、例えば、信頼性の低い経路を経由したと判定した場合には、以降のセッションを中止するといった処理を行うことが可能である。
【００６１】
次に、シグナリングプロトコルとしてＳＩＰを用いる場合の各装置の機能ブロックを図８を参照して説明する。
【００６２】
セッション管理サーバは、呼（メッセージ）の転送のための処理を行うＳＩＰプロキシ、ＳＩＰの名前登録を行うＳＩＰレジストラ、ＩＤ、パスワード、もしくは証明書等を用いて各端末の認証を行う認証モジュール、ＩＰｓｅｃ等の暗号化通信を行うための暗号化モジュールを有している。
【００６３】
また、各端末は、セキュアデータチャネル上での通信を行う機能部、ＩＮＶＩＴＥメッセージの送受信やＲＥＧＩＳＴＥＲメッセージの発行等を含むＳＩＰに基づくメッセージ通信を行うＳＩＰ機能部、ＩＤ、パスワード、もしくは証明書等を用いてセッション管理サーバの認証を行う認証モジュール、ＩＰｓｅｃ等の暗号化通信を行うための暗号化モジュールを有している。
【００６４】
上記のセッション管理サーバ、各端末の機能は、プログラムにより実現されるものであり、本発明におけるセッション管理装置、端末の各手段は、プログラムと、セッション管理装置、端末のハードウェアとで実現されているものである。また、端末は、ＣＰＵ、メモリ、ハードディスク等を含む一般的なＰＣ等のコンピュータ、モバイル機器等であり、当該コンピュータ等に上記プログラムをインストールすることにより本実施の形態の端末の機能を実現できる。なお、端末はディジタル家電等でもよい。また、セッション管理サーバは、サーバ等のコンピュータであり、ＣＰＵ、メモリ、ハードディスク等を含む。当該サーバに上記プログラムをインストールすることにより本実施の形態のセッション管理サーバの機能を実現できる。
【００６５】
上記のように本実施の形態のような構成としたことにより、次のような効果を奏する。

【００６６】
まず、端末のアドレスが変更される度にＲＥＧＩＳＴＥＲメッセージによる名前とＩＰアドレスの登録を行うので、端末側はいわゆる動的ＩＰアドレス割り当てを用いることができる。また、セッション管理サーバが名前解決を行うことから、従来は必要であったオープンなＤＮＳへの名前登録が不要となる。また、各端末とセッション管理サーバ間でセキュアなチャネルを構築してシグナリングを行うので、端末側でのＦＷ管理が不要となる。また、セッション管理サーバが各端末のＩＤ、パスワードを管理するので、端末側で多数のＩＤ、パスワードを管理することが不要となる。また、セッション管理サーバ接続ポリシー制御機能により、接続を許可していない相手端末に対しては、名前解決さえ許可していないので、その端末の存在自体を知られることがなく、端末が不正なアクセスを受ける恐れがなくなる。更に、セキュアシグナリングチャネルを介したシグナリングにより、セキュアデータチャネルに必要なポート番号が伝えられるので、シグナリングが正常に完了しない場合には、外部にはポート番号を知られることがない。また、軽いシグナリングだけが中間サーバ（セッション管理サーバ）を経由し、実際のデータ通信は端末間でピア・ツー・ピアで行われるので、中間サーバの負荷が過大となることはない。

【００６７】
また、従来技術においては、多数の端末同士の間で相互認証および暗号化されたピア・ツー・ピアの通信を行うためにはそれら全端末の証明書を取得するか、あるいは全端末のＩＤ、パスワードを管理することが必要であったが、本発明によれば、メンバー同士であれば何の事前セキュリティ設定が不要となる。

【００６８】
また、従来技術において、データチャネルの暗号化が不要だったとしても、発番号の信憑性を確保する手段として、PKIを使う方法等しかなかったが、本発明によれば、サービス設定（SIPのID/パスワード設定）だけで発番号の詐称・改竄を防ぐことができる。

【００６９】
更に、ＩＮＶＩＴＥメッセージにおけるＦｒｏｍ行の内容の確認を行うことにより、ＩＮＶＩＴＥメッセージの発信元が名前の詐称をしていないかどうかを確認できるようになり、より信頼性を向上させることが可能となる。更に、Route-Securityヘッダを用いることにより、経路の安全性を確認することができ、更に信頼性を向上させることが可能となる。なお、SIPサーバに接続してくる者が必ずしもセキュアなチャネルを通ってきていない場合があることを前提とした場合、名前の詐称確認及びRoute-Securityヘッダによる経路の安全性確認を行うことにより、セキュリティを確保した通信を実現できる。

【００７０】
また、実施の形態で説明した詐称確認、Route-Securityヘッダを用いたしくみを用いることにより、他のネットワークを介した場合でも、端末―端末間のセキュアな通信が可能となる。

【００７１】
なお、詐称確認、Route-Securityヘッダを用いたしくみをINVITEメッセージを例にとって説明したが、INVITEメッセージに限られるものでなく、種々のメッセージ転送に適用できる。

【００７２】
本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【図面の簡単な説明】

【００７３】
【図１】本発明の実施の形態の概要について説明するための図である。
【図２】端末１－セッション管理サーバ３－端末２間の通信のシーケンス図である。
【図３】シーケンスを詳細に示す図である。
【図４】ＲＥＧＩＳＴＥＲメッセージのシーケンスを示す図である。
【図５】身元詐称監視、及びRoute-Securityヘッダを説明するためのシーケンスチャ

ートである。
【図６】図５のシーケンスを説明するための図である。
【図７】図５のシーケンスを説明するための図である。
【図８】シグナリングプロトコルとしてＳＩＰを用いる場合の各装置の機能ブロック図である。

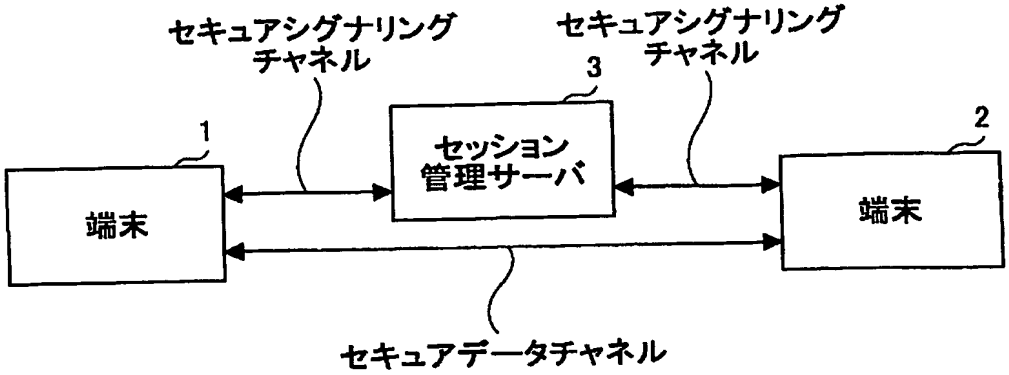
【符号の説明】

【００７４】

１、２　端末
３、Ａ、Ｂ　セッション管理サーバ

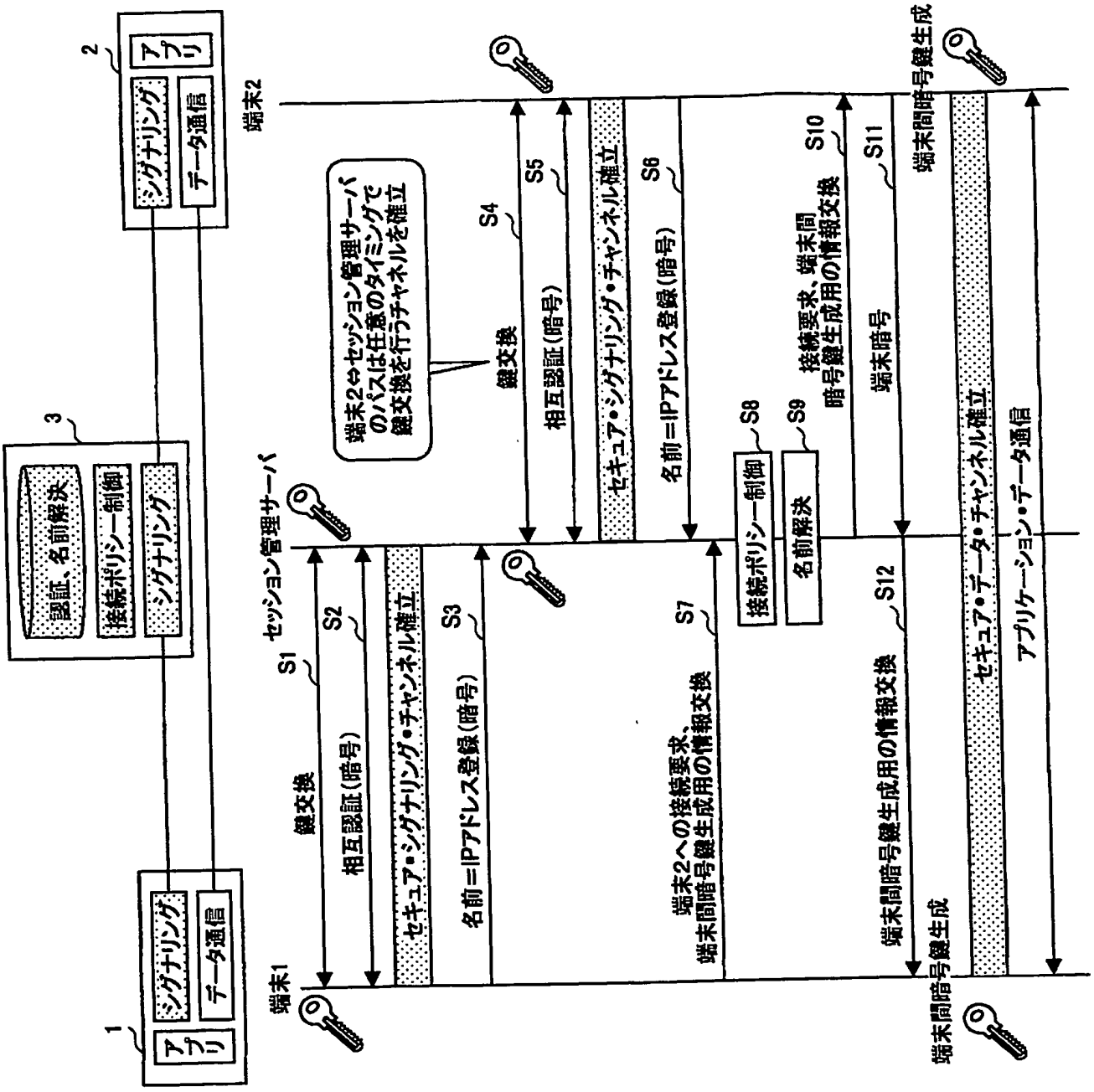
【書類名】図面
【図１】

本発明の実施の形態の概要について説明するための図



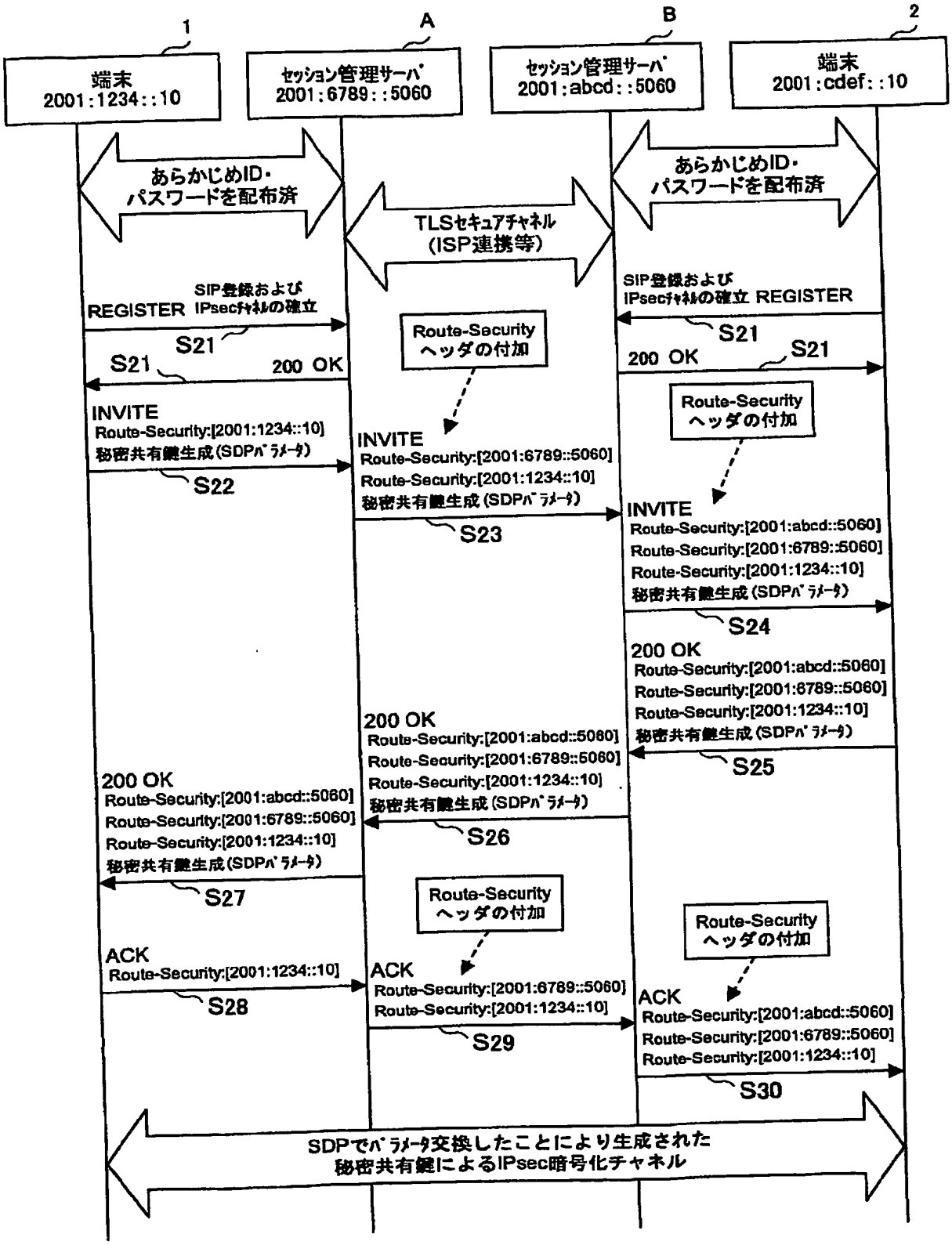
【図２】

端末1－セッション管理サーバ3－端末2間の通信のシーケンス図



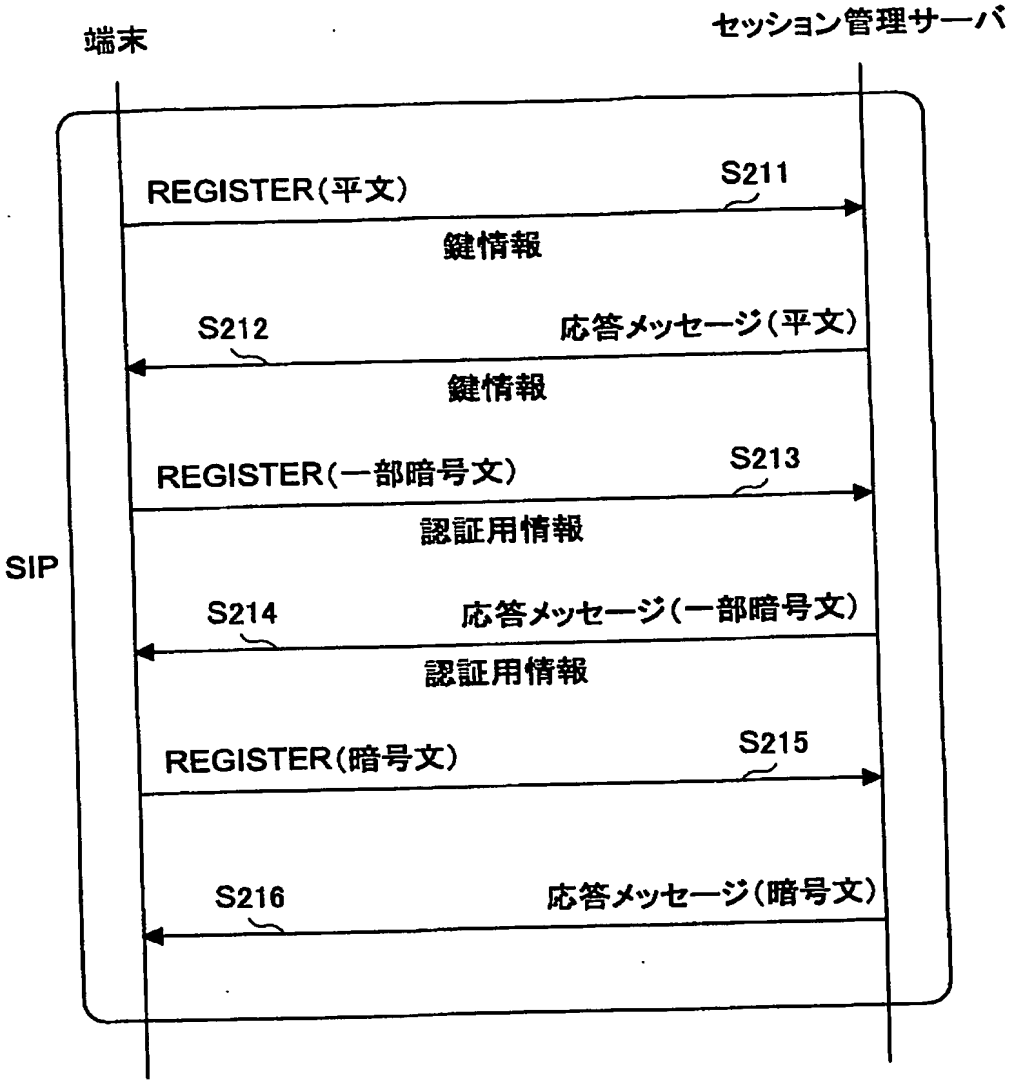
【図３】

シーケンスを詳細に示す図



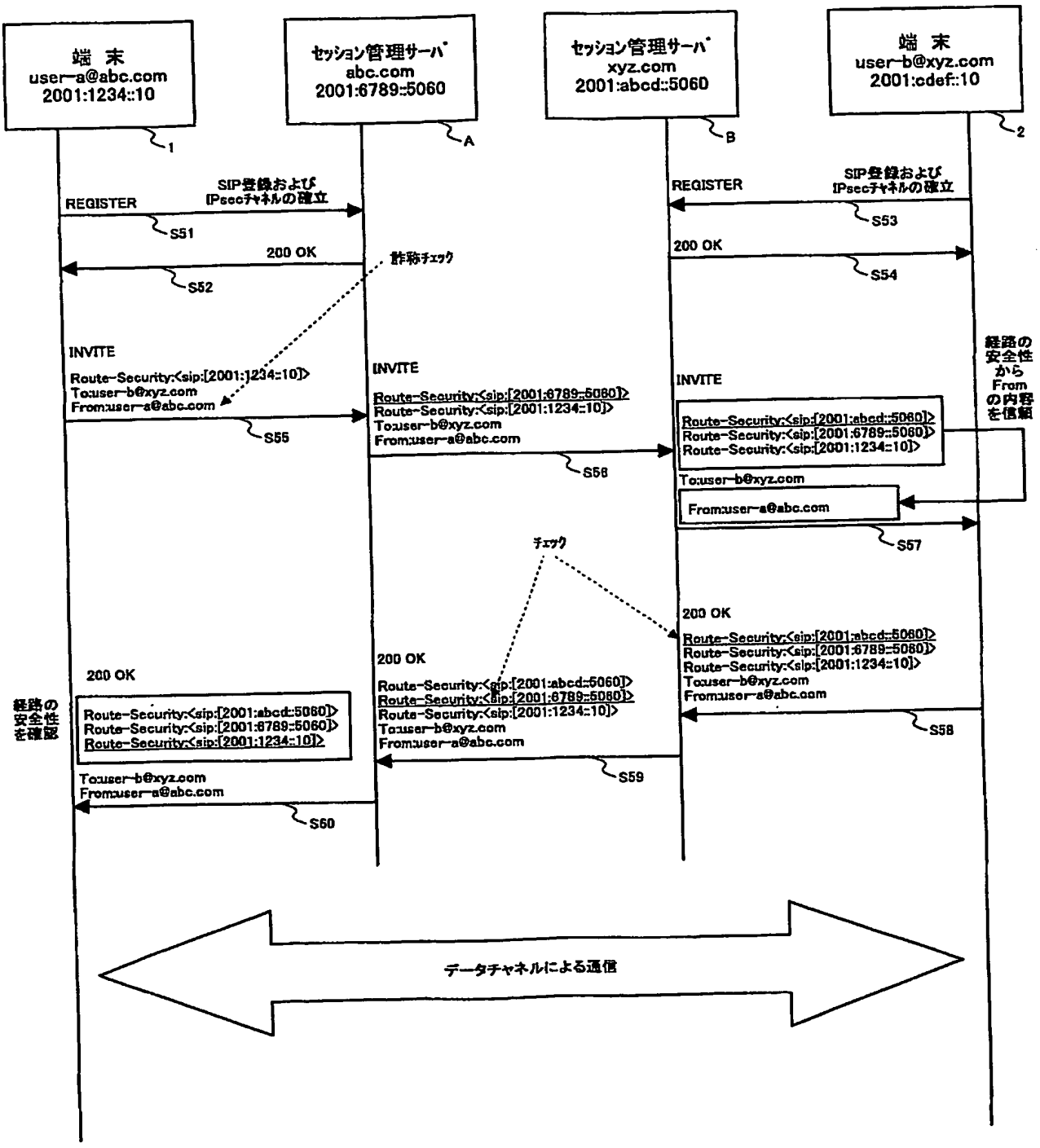
【図４】

REGISTERメッセージのシーケンスを示す図



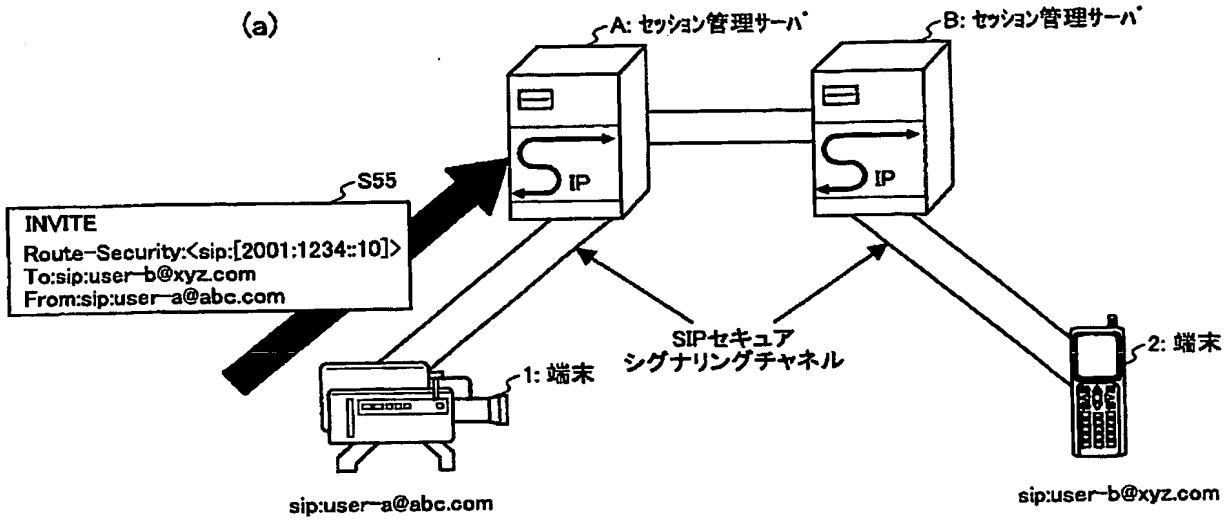
【図５】

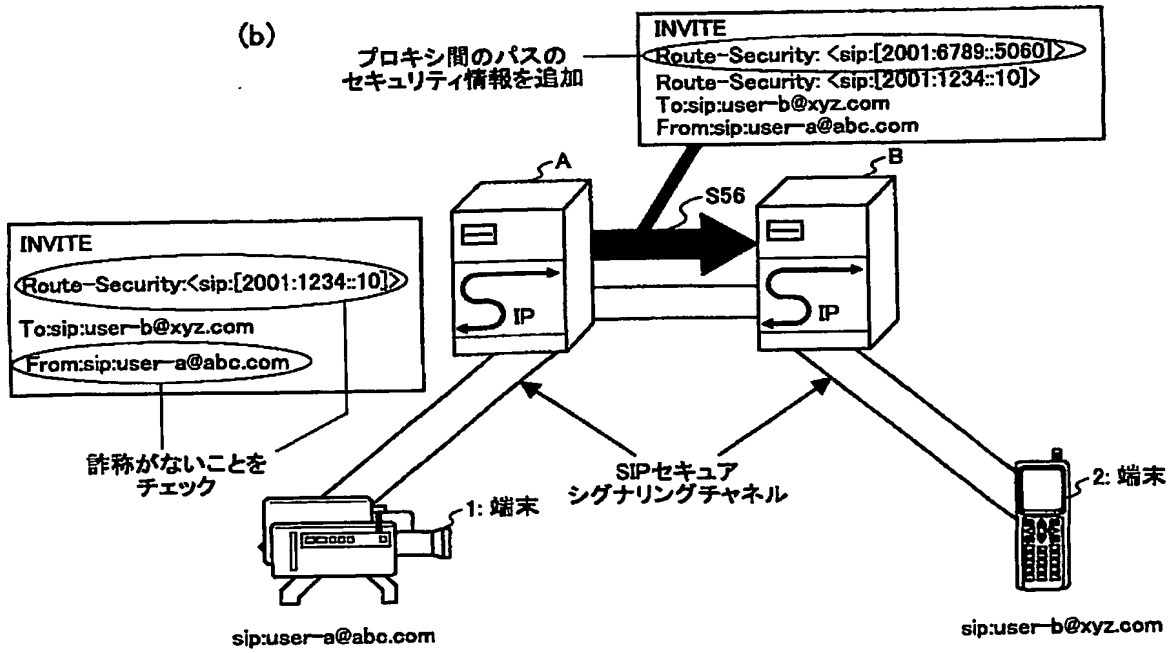
身元詐称監視、及びRoute-Securityヘッダを説明するためのシーケンスチャート



【図６】

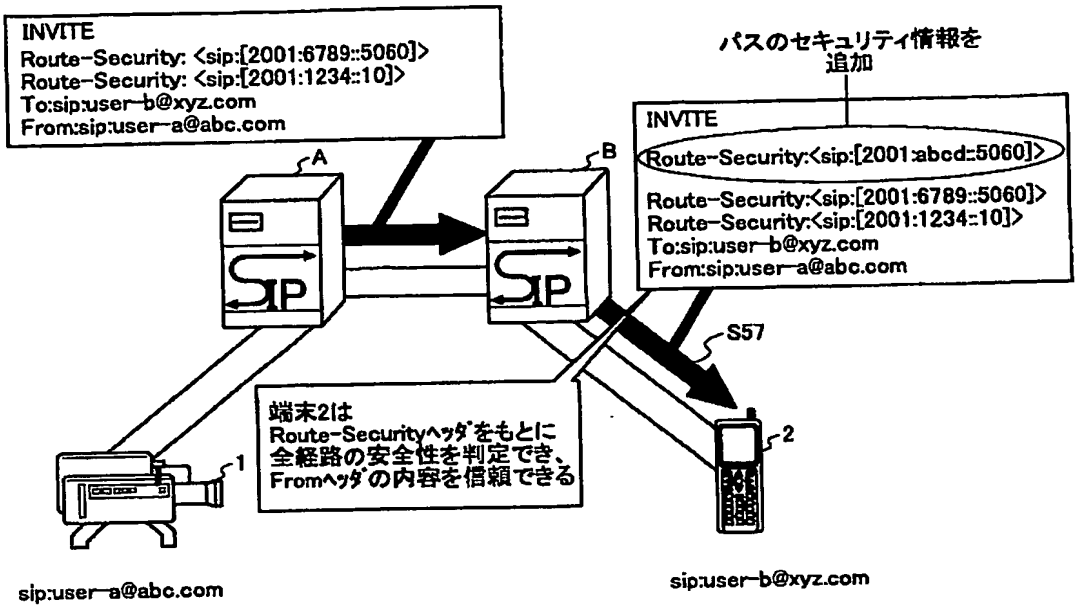
図5のシーケンスを説明するための図

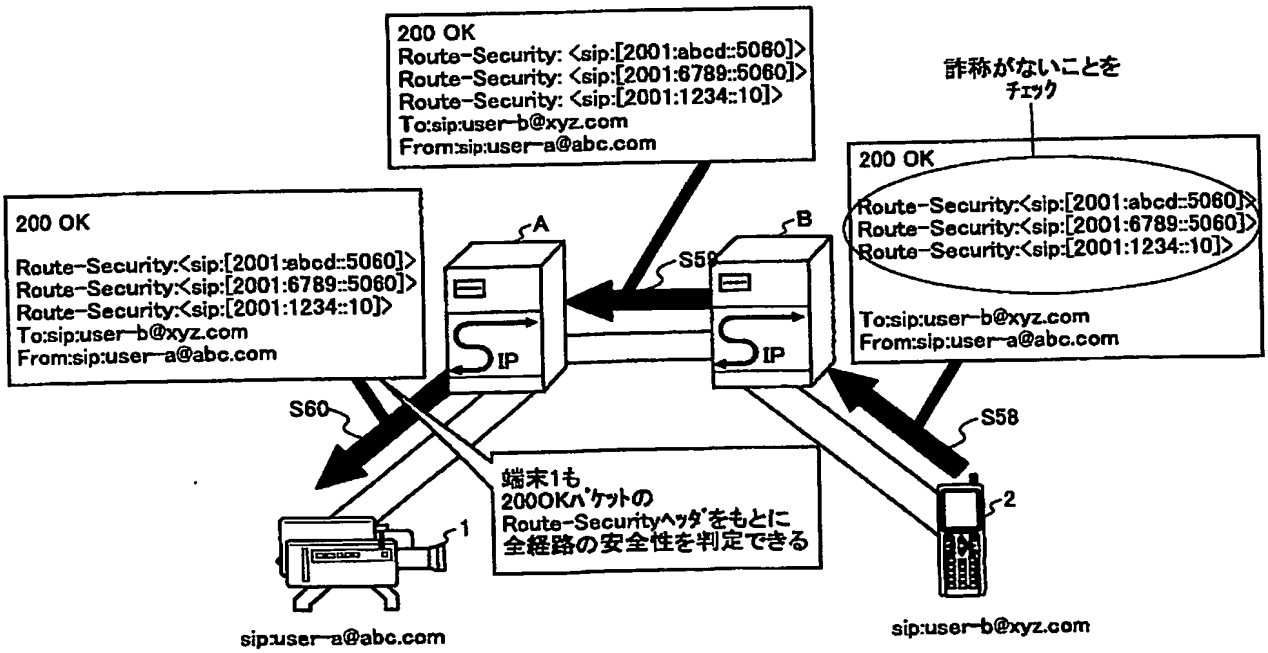




【図７】

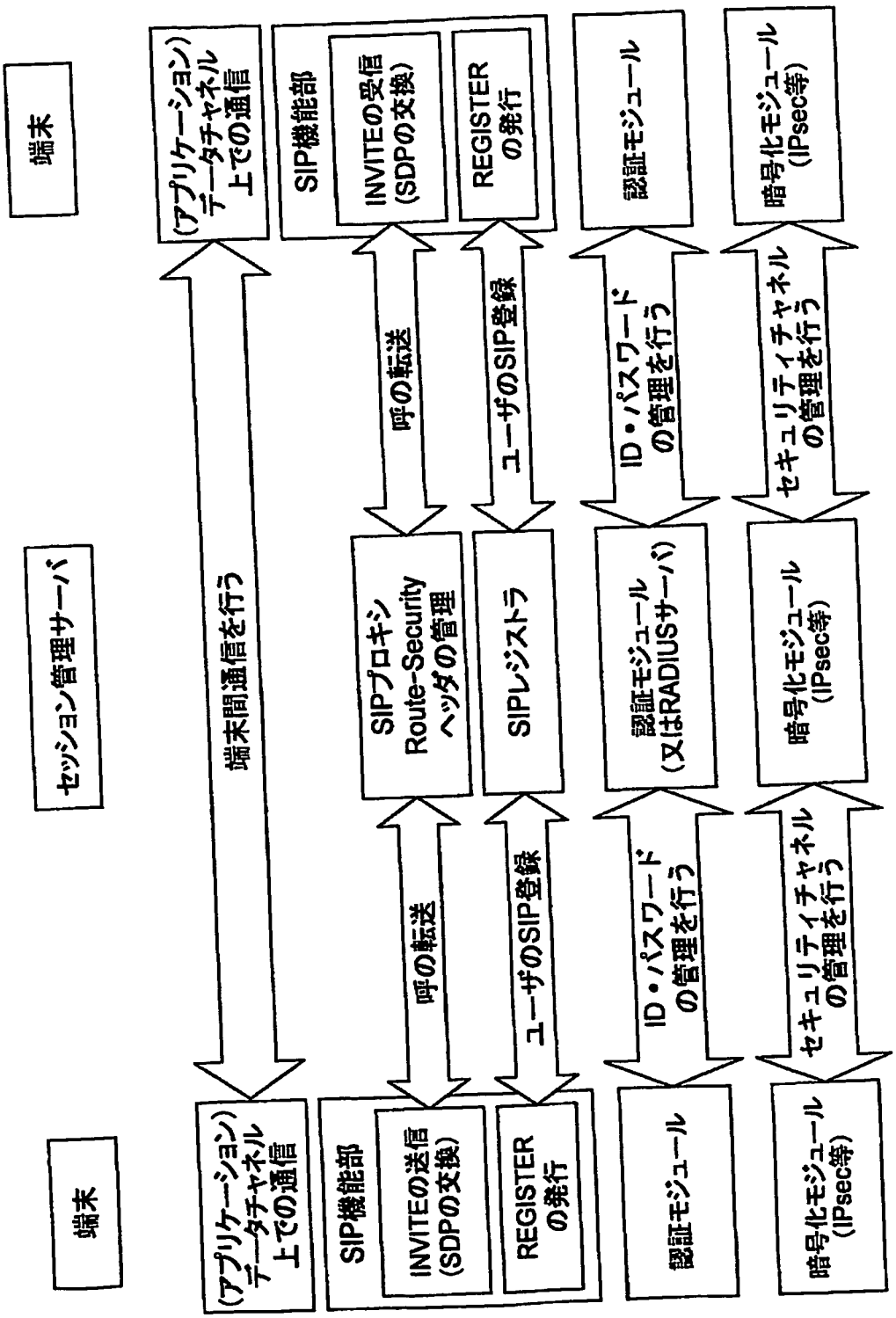
図5のシーケンスを説明するための図





【図８】

シグナリングプロトコルとしてSIPを用いる場合の各装置の機能ブロック図



【書類名】要約書
【要約】
【課題】　安全にシグナリングを行って、端末間でセキュアなデータチャネルを容易に構築する。
【解決手段】　第１の装置及び第２の装置とネットワークを介して接続する手段を備えたセッション管理装置において、第１の装置との間で相互認証を行い、セッション管理装置と第１の装置との間で第１の暗号化通信チャネルを確立し、第１の装置の名前と第１の暗号化通信チャネルの識別情報とを対応付けて保持する手段と、セッション管理装置と第２の装置との間で相互認証に基づく第２の暗号化通信チャネルを確立する手段と、第１の装置から、第１の装置の名前を含むメッセージを、第１の暗号化通信チャネルを介して受信し、当該メッセージに含まれる第１の装置の名前と、第１の暗号化通信チャネルの識別情報と対応付けて保持されている第１の装置の名前とを比較することにより、メッセージに含まれる第１の装置の名前が正しいか否かを判定する手段と、そのメッセージを第２の暗号化通信チャネルを介して第２の装置に送信する手段とを備える。
【選択図】　図１

特願２００４－０３７３１４

出　願　人　履　歴　情　報

識別番号　　［３９９０３５７６６］

１．変更年月日　　１９９９年　６月　９日
［変更理由］　　新規登録
住　所　　東京都千代田区内幸町一丁目１番６号
氏　名　　エヌ・ティ・ティ・コミュニケーションズ株式会社